



Protecting  
Your Digital  
Assets

# CRU® User Manual

## RAX® Secure 3QR



### Features

- Disk setup is near-instantaneous and is capable of JBOD, RAID 0 and 1 disk modes.
- Hardware-based AES 256-bit Encryption--Offers affordable military-grade AES 256-bit data protection that encrypts the entire hard drive--including boot sector, OS, and swap files.
- eSATA, FireWire 800, USB 2.0, and USB 3.0 connections are provided for wide variety of connectivity.
- Specially designed drive and carrier interfaces are built to withstand tens of thousands of insertions.

## Table of Contents

1. Pre-Installation Steps	2
1.1 Box Contents	2
1.2 Identifying Parts of your RAX800-TR	2
1.3 Warnings and Notices	2
2. Introduction to RAID	3
2.1 Summary of RAID Levels	3
3. Installation Steps	3
3.1 Installing Hard Drives	3
3.2 Host Connections	3
3.3 Operating Your RAX 3QR Unit	3
4. LED Behavior	4
5. LCD Menu Screens	4
6. RAID Configuration	4
6.1 Creating a New RAID	4
6.2 Changing the RAID Type	4
6.3 Adding a New Drive to a RAID	5
7. Usage with Mac and Windows Operating Systems	5
7.1 Usage with Mac OS X	5
7.1.1 Formatting a Drive	5
7.1.2 Mounting and Unmounting Volumes	5
7.1.3 Creating a Boot Drive	5
7.2 Usage with Windows Operating Systems	5
7.2.1 Formatting a Drive	5
7.2.2 Mounting and Unmounting Volumes	6
8. Buzzer and Temperature Configuration	7
8.1 Accessing the RAX 3QR Unit's Settings	7
8.2 Customizable Options	7
9. RAID Is Not A Backup	7
10. Encryption	8
11. Rack Mounting Warnings	8
12. Frequently Asked Questions	8
13. Technical Specifications	10

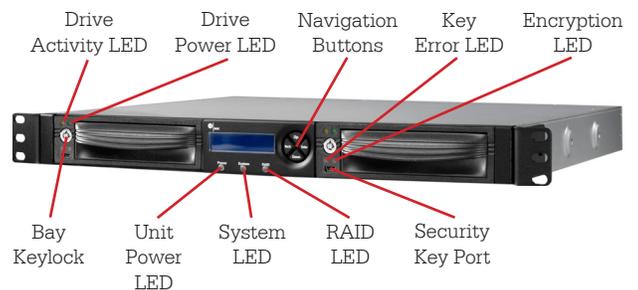
## 1. Pre-Installation Steps

### 1.1 Box Contents

The following list contains the items that are included in the complete configuration for this device. Please contact CRU if any items are missing or damaged:

Accessories	Quantity
RAX 3QR Unit	1
Power Cord	1
Key Set	1
Screw Kit	1
Security Key	3
Lanyard for Security Key	3
Security Key ID Tag	3
Security Key Label	3
Quick Start Guide	1

### 1.2 Identifying Parts of your RAX 3QR Enclosure



### 1.3 Warnings and Notices

Please read the following before beginning installation.

#### General Care

- Proper grounding is strongly recommended to prevent electrical damage to the unit or other connected devices, including the computer host. Avoid all dramatic movement, tapping on the unit, and vibration.
- Avoid placing the unit close to magnetic devices, high voltage devices, or near a heat source. This includes any place where the product will be subject to direct sunlight. Do NOT allow water to make contact with the unit.
- Before starting any type of hardware installation, please ensure that all power switches have been turned off and all power cords have been disconnected to prevent personal injury and damage to the hardware.

- To avoid overheating, the unit should be operated in a well-ventilated area.
- Remove the drives before transporting the unit to prevent damage to the drive interfaces.

## RAID

- Use only hard drives that are in perfect condition. Avoid using drives that have ever developed bad sectors during previous usage. This could lead to possible device failure or loss of data.
- The unit supports SATA hard drives of various specifications and different capacities. However, we recommend using drives of the same brand and type for optimal performance. If drives of different capacities are used in a RAID, the capacity of the smallest drive will determine how much of each drive is used. The additional capacity on the larger drives will not be used by the RAID.
- RAID level 0 will allow you to use the full combined capacity of the drives, and offers the best data transfer speeds. However, RAID 0 offers no protection for the data. If one drive fails in a RAID 0, the data on all of the drives is irretrievably lost. Before creating a RAID, investigate the various RAID types and choose the one that is best for your needs.
- Always back up data before switching RAID types. **Switching RAID types will destroy current data.** You must reformat your drives afterwards.

## Encryption

- Though the Security Key port is mechanically identical to the standard Mini-USB port, inserting Security Keys into any other Mini-USB port may damage the keys and render them useless. Please only use Security Keys in RAX products.

Likewise, inserting a Mini-USB cable or other device into the unit's Security Key port on the carrier may cause internal damage and potentially lead to loss of data.

- Any time power is cycled on the unit, the Security Key should be installed prior to recycling the power in order to access the data on the drive.

## 2 Introduction to RAID

A RAID (Redundant Array of Independent Disks) is an array of multiple hard drives that are combined in a way that provides faster performance and/or data safety. Your RAX Secure 3QR unit is capable of creating and managing several different varieties of RAID. You may choose your preferred RAID level based on factors such as disk capacity, desired data safety, and desired performance.

## 2.1 Summary of RAID Levels

RAX Secure 3QR units support JBOD and RAID Levels 0 and 1. RAID Level 1 is used by those seeking data safety.

RAID Level	Description	Required No. of Drives*	Fault Tolerance
JBOD	Known as "Just a Bunch Of Disks". This is not a type of RAID as each disk is created with its own independent volume. There is no data protection.	1	No data protection
0	Also known as striping. Data distributed across all drives in the array. There is no data protection.	2	No data protection
1	Also known as mirroring. All data replicated on two separate disks. Due to the 100% duplication, only half the total disk capacity is available for data storage.	2	1 drive

## 3 Installation Steps

### 3.1 Installing Hard Drives

- Slide the drive carrier out of the RAX enclosure.
- The carrier's cover is held in place by a screw on the rear of the unit. Remove the screw and then remove the cover.
- Slide the drive in from the front of the carrier.
- Mate the connection on the drive with the connection on the drive carrier circuit board.
- Flip the drive/carrier assembly over and secure the drive in place with the provided screws.
- Attach the Temperature Control Cooling Sensor to the top of the drive with a piece of tape.
- Replace the carrier cover and secure the screw on the rear of the carrier.
- Slide the carrier into the RAX enclosure.

### 3.2 Host Connections

RAX Secure 3QR units connect to your computer in one of four ways; USB 3.0, USB 2.0, Firewire 800, or eSATA. Choose one of the four cable types to use and plug it into the unit. Each bay requires its own data connection.

### 3.3 Operating Your RAX Secure 3QR unit

- Connect the data cables to the RAX enclosure and to your computer.
- Plug in the power cord to the RAX enclosure and to a grounded electrical outlet.
- If you have not already done so, slide the carriers into the open receiving frames on the RAX Secure 3QR unit.
- Insert the Security Key into the Mini-USB Security Key

Port on the face of each receiving frame.

- e. Insert a DataPort key into the key lock and turn it 90 degrees clockwise to power on the unit.
- f. When both green LEDs are lit on both receiving frames, showing that the drives are ready and encryption is activated, remove the Security Key and store it in a safe location.

When any hard drive is first used with a RAX Secure enclosure, it will show up as a blank, unallocated drive and you'll need to add it to a RAID before you can use it. **Note that adding a drive to a RAID will erase all data on the drive, so be sure to back up your data before beginning this operation.**

#### 4 LED Behavior

LED Name	Color	State	Description
Unit Power	Green	Solid	RAX Secure 3QR unit is powered on
System	Green	Solid	System is performing as expected
	Amber	Solid	Drive has reached the preset warning temperature
	Red	Solid	Fan has stopped rotating or the drive has reached the preset alarm temperature
RAID	Green	Solid	RAID is performing as expected
	Amber	Solid	RAID is degraded or is being rebuilt
	Red	Solid	RAID has failed or is invalid
Drive Power	Green	Solid	Bay is powered on
		Flashing	Indicates a bay fan failure
Drive Activity	Pink	Intermittent	Flashes when the drive inside is being accessed
Key Error	Red	Solid	Encryption engine error. Contact Technical Support.
		Flashing	The Security Key is not present or is not functioning.
Encryption	Green	Solid	The Security Key is present and encryption is enabled
		Off	Encryption is disabled

#### 5 LCD Menu Screens

Screen	Description
Mode	Shows the RAID level used.
Status	Indicates the overall health of the RAID. Available status messages are "Normal" and "Degraded".
Disk#	Indicates the status of the individual disk in the numbered bay: <ul style="list-style-type: none"> <li>• OK: Indicates that the hard drive is in use or ready to use</li> <li>• No Disk: Indicates that the hard drive was removed or not installed</li> <li>• Unused: A new drive was installed and is not used by the RAID.</li> <li>• Failing: Indicates the drive is malfunctioning. Possible causes of a failure message include an inability to recognize the drive, a compatibility problem, or damaged sectors.</li> </ul>

Disk# Temp	Displays temperature of the individual disk in the numbered slot.
Sys Temp	Displays the overall temperature inside the system
Fan Status	Indicates whether the fan is operating normally or has failed and is in need of a replacement. Contact Technical Support if the fan has failed to arrange for a repair.
Change RAID Mode	Allows you to change the RAID level (See Section 6.2).

#### 6 RAID Configuration

Use the LCD and menu selection buttons to complete these steps. **Changing RAID levels will erase any data on the drives. Make a backup copy of any data you wish to keep before changing the RAID.**

##### 6.1 Creating a New RAID

- a. Disconnect the RAX Secure 3QR unit from the computer.
- b. Power on the RAX Secure 3QR unit using the steps detailed in Section 3.3
- c. After the RAX Secure 3QR unit boots up, it will begin alarming and the LCD will display the error "Error: Not a RAID Set". Press the **Enter** button to silence the alarm.
- d. Press the **Enter** button a second time and the LCD screen will ask "Make New RAID?" Press **Enter** to confirm.
- e. The LCD will display "Select RAID Type". Press **Up** or **Down** to cycle through to your desired RAID type and press **Enter**.
- f. The screen will display "Will Erase all Data OK?" **Pressing Enter will result in the loss of all data on the drives.** Ensure all data is backed up, then press **Enter**.
- g. The new configuration will be selected and the RAX Secure 3QR unit will reboot. The RAID is now created.

##### 6.2 Changing the RAID Type

- a. Disconnect the RAX Secure 3QR unit from the computer.
- b. Press the **Up** button to cycle the LCD menu to the "Change RAID Mode" screen and press the **Enter** button.
- c. The LCD will display "Select RAID Type". Press **Up** or **Down** to cycle through the available options to your desired RAID type and press **Enter**.
- d. The screen will display "Will Erase all Data OK?" **Pressing Enter will result in the loss of all data on the drives.** Ensure all data is backed up, then press **Enter**.

- e. The new configuration will be selected and the RAX Secure 3QR unit will reboot. The RAID is now created.

The RAX Secure 3QR unit has been configured and is ready for operation. Follow the appropriate operating system usage instructions in Section 7 to initialize and format the drives.

### 6.3 Adding a New Drive to a RAID

**NOTE:** Any data on the new hard drive will be destroyed when the drive is added to the RAID

#### RAID 0

Never remove a drive from a RAID 0 as this will cause the loss of all data. In the event of a disk failure for a RAID 0, the RAID will be destroyed. Add a drive and then press the Up button to create a new RAID. Follow the display prompts to build a new array.

#### RAID 1

In the event of a disk failure or removal, the RAID will continue to function in a degraded state. Add a new disk to the RAX Secure 3QR unit to rebuild the RAID. After the new drive has been detected, the RAX Secure 3QR unit will ask to add a new disk. Press the Enter button to do so. The disk will be added to the RAID and the RAID will begin to rebuild. The LCD screen will display the percent complete for the rebuild. Rebuild times vary, but a 1TB hard drive typically takes just over 3 hours to rebuild. You can toggle to the approximate time remaining by pressing Enter on the front panel.

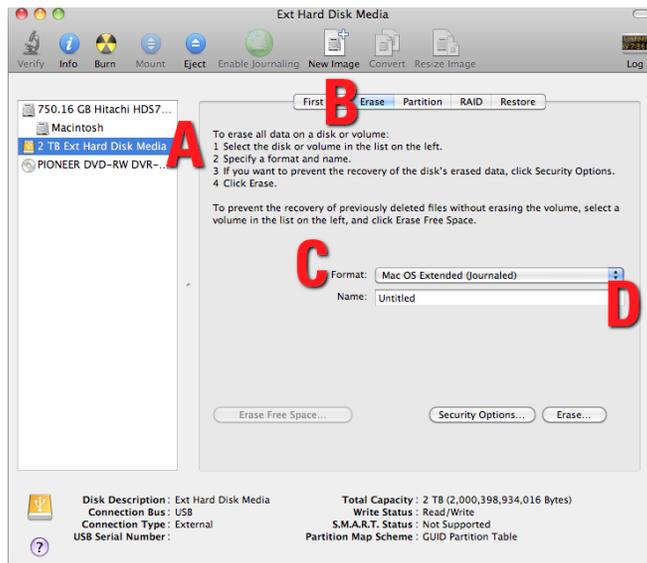
## 7 Usage with Mac and Windows Operating Systems

### 7.1 Usage with Mac OS X

#### 7.1.1 Formatting a Drive

To format, use Disk Utility (pictured below), which can be found in the Applications folder.

- Click on the drive in the window to the left.
- Click the **Erase tab** in the window to the right.
- Select the format type. Most users prefer **Mac OS Extended with Journaling (HFS+)**, which is required for compatibility with Time Machine (OS 10.5 or newer). If you need to use your RAX Secure 3QR unit with both Mac and Windows computers, select **MS-DOS File System** instead.
- Enter a name for the new volume and then click **Erase** to start the process.



#### 7.1.2 Mounting and Unmounting Volumes

If the hard drive installed in the RAX Secure 3QR unit is already formatted, an icon representing the drive's volume will appear (mount) on the desktop. You can begin using the volume right away. If the drive is unformatted, a message will appear on the desktop saying that the disk is unreadable. Use OS X's Disk Utility to easily format the drive (see section above).

Unmount the volume before powering down the unit by dragging the volume's icon to the **Trash**, or by selecting the volume then pressing **Command-E**. Disconnecting the unit without first unmounting the volume can result in data loss.



#### 7.1.3 Creating a Boot Drive

To activate this feature, you must first install OS X on the hard drive in your carrier. The easiest way to do this is to clone an existing system drive using a utility such as Carbon Copy Cloner or Super Duper. Next, go to **System Preferences** → **Startup Disk**. A window will list the available bootable volumes. Select the volume from which you wish to boot. Another method is to hold down the **Option key** during boot up. A screen should appear that allows you to select the volume you wish to use. This is useful if you are only sporadically booting from the RAX Secure 3QR unit hard drive.

### 7.2 Usage with Windows Operating Systems

#### 7.2.1 Formatting a Drive

When you first mount a drive to a Windows operating system, a pop-up window will ask you if you would like to format it. Click **Format Disk** and skip to Step E. If the prompt does not pop up, use the Disk Management utility by following these steps:

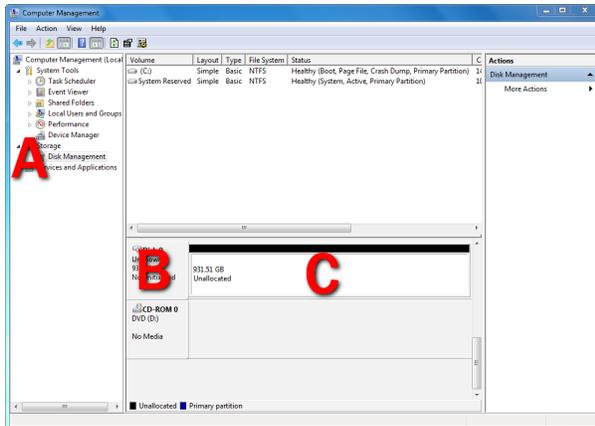
- Right-click on the **My Computer icon** on the

desktop (Windows XP) or the **Computer button** in the Start Menu (Windows Vista, 7, Server 2008 and 2012 product families), then select **Manage**. In the left pane of the Computer Management window that opens, left-click on **Disk Management** (labeled 'A' in the picture below). For Windows 8.1, press **WINKEY + X**, then select **Disk Management** from the menu that pops up.

- b. The drive should appear in the list of Disks in the lower pane. You may need to scroll down to see it. If the drive is already formatted, you can identify it easily by its volume name. If the Device Properties Box (labeled 'B' in the picture below) says "Not Initialized", you'll need to initialize the disk before formatting it.

Right-click on the **Device Properties Box** and select **Initialize Disk**. If you are prompted to select a partition type, select **GPT**. Only select **MBR** if you are formatting a bootable disk for use on a system with a legacy BIOS or are using the RAX Secure 3QR unit with Windows XP.

- c. To format the volume, right-click the **Drive Properties Box** (labeled 'C' in the picture below) and select **New Partition...** (Windows XP) or **New Simple Volume...** (Windows Vista, 7, 8.1, Server 2008 and 2012 product families).



- d. Unless you wish to customize the settings in these dialog prompts, click **Next** on the Select Partition Type (shows up in Windows XP only), Specify Volume/Partition Size, and Assign Drive Letter or Path dialog prompts, leaving the default settings.
- e. You will now see a window that allows selection of a file system. Choose **NTFS** and enter a name for the new volume. Be sure to check the box labeled **Quick Format**, which will ensure that the formatting process takes less than a minute.
- f. Click **Next** and then **Finish** to start the format process. When the format is complete, the Drive

Properties Box will update to show the new volume name. The new volume can now be found by double-clicking on the **My Computer icon** on the desktop (Windows XP), by clicking on the **Computer button** in the Start Menu (Windows Vista, 7, Server 2008 product family), by clicking on **Computer** in the navigation pane of a File Explorer window (Windows Server 2012), or by opening a File Explorer window (Windows 8.1, Server 2012 R2).

## 7.2.2 Mounting and Unmounting Volumes

If the hard drive inside of the RAX Secure 3QR unit are already formatted, you can begin using the volume right away. When the RAX Secure 3QR unit is properly connected and turned on, a window may open to allow you access to the volume. If no window appears, find the volume by double-clicking on the **My Computer icon** on the desktop (Windows XP), by clicking the **Computer button** in the Start Menu (Windows Vista, 7, Server 2008 product family), by clicking on **Computer** in the navigation pane of a File Explorer window (Windows Server 2012), or by opening a File Explorer window (Windows 8.1, Server 2012 R2).

### Unmounting a USB or Firewire Volume

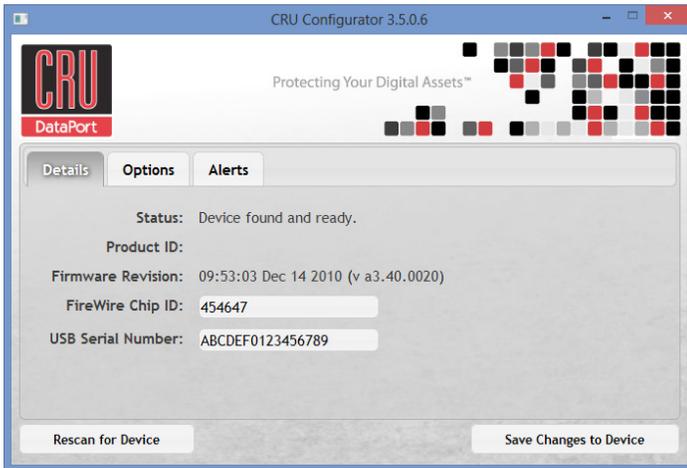
Unmount the RAX Secure 3QR unit before powering it down by left-clicking the **green arrow icon** on the task bar (in Windows XP) or the **USB plug icon** with the green checkmark on the Desktop task bar (Windows Vista, 7, 8.1, Server 2008 and 2012 product families), and then selecting the proper device from the menu that pops up. You may have to click on the **Show Hidden Icons arrow** on the task bar to find the correct icon. Windows will indicate when it is safe to disconnect the RAX Secure 3QR unit. Disconnecting the RAX Secure 3QR unit without first ejecting it can result in data loss.



### Unmounting an eSATA Volume

If you purchased an eSATA host card that supports hot-swapping, follow the instructions for unmounting a USB or FireWire volume above. Many eSATA hosts do not support this feature. However, freeware utilities are available on the Internet that provide a similar function. You may download one of these utilities or follow these instructions: Ensure no file transfers are taking place by making sure the Bay Access/Drive Activity LEDs are not blinking, as disconnecting the unit while a file transfer is in progress can result in data loss. Then disconnect power to the RAX Secure 3QR unit. You may need to restart your computer in order to remount the RAX Secure 3QR unit.

## 8 Buzzer and Temperature Configuration

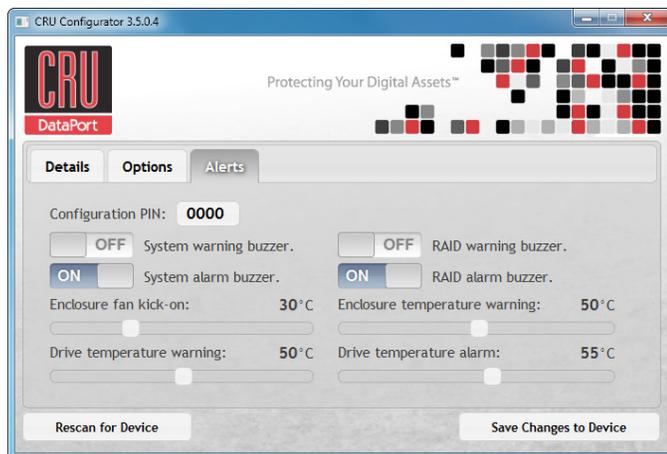


The RAX Secure 3QR unit is compatible with CRU Configurator 3.5 or higher, which allows IT administrators to change internal settings to meet individual needs. Configurator allows the user to set the password, enable and disable audible alarms, and change temperature alarms and warnings settings. To download Configurator and the full Configurator manual, visit [cru-inc.com/support/software-downloads/configurator-software-download/](http://cru-inc.com/support/software-downloads/configurator-software-download/).

### 8.1 Accessing the RAX Secure 3QR Unit's Settings

Connect a FireWire 800 cable to either FireWire port or use a USB Type A-to-A cable (both cables sold separately) in the USB/eSATA combo port. Then open Configurator.

### 8.2 Customizable Options



The following options are available on the Alerts tab of the Configurator:

#### Configuration PIN

This feature allows you to set a PIN to prevent unauthorized configuration. The default PIN is 0000. The RAX Secure 3QR unit only requires you to enter a PIN if a different value has been set.

#### Buzzers

Place a check in the boxes to indicate which warning/alarm buzzers you want to be activated or remove a check from

the boxes next to the buzzers you want to deactivate. When a buzzer sounds, press Enter on the front of the RAX Secure 3QR unit to temporarily silence it until the RAX Secure 3QR unit is next rebooted.

#### System Warning Buzzer

This buzzer will sound when a drive reaches the temperature set using the Drive temperature warning slider below. This buzzer is disabled by default. As a visual alert, the System Status LED will glow amber when the temperature is reached, regardless of whether the buzzer is enabled or not.

#### System Alarm Buzzer

This buzzer will sound on 3 occasions:

- When a drive reaches the temperature set using the Drive temperature alarm slider below
- When the unit reaches the temperature set using the unit temperature warning slider below
- When the fan fails

As a visual alert, the System LED on your RAX Secure 3QR unit will glow red when any of these three situations occur, regardless of whether the buzzer is enabled or not.

#### RAID Warning Buzzer

This buzzer will sound when the RAX Secure 3QR unit is in degraded RAID mode (a drive has failed and is in need of rebuild or the RAID is rebuilding). This buzzer is disabled by default. The RAID LED will glow amber if this occurs, regardless of whether the buzzer is enabled or not.

#### RAID Alarm Buzzer

This buzzer will sound when the RAID has failed or is invalid. The RAID LED will glow red if this occurs, regardless of whether the buzzer is enabled or not.

#### Temperature Sliders

When your RAX Secure 3QR unit reaches a certain temperature, buzzers will sound if they are enabled (see the Buzzers subsection above) and the fan will kick on. You may want to change these default temperatures according to your environment. With these sliders, you can change the default temperatures of the following features:

- Unit fan kick-on
- Unit temperature warning
- Drive temperature warning
- Drive temperature alarm

## 9 RAID Is Not A Backup

Because your RAX Secure 3QR unit features redundant RAID modes which protect against a hard drive mechanical failure, it is an excellent part of any backup strategy. However, a RAID is not, in itself, a backup strategy. Many things besides hard drive failure can damage or erase your data:

- Corruption caused by unexpected disconnection during data access (e.g. a cable is unplugged during a data

transfer, or the computer crashes or loses power while writing to the drives)

- Corruption or destruction caused by viruses or other malware
- Sabotage by a disgruntled employee or acquaintance
- Theft of your RAX Secure 3QR unit
- Natural disasters such as fire, flooding, etc.

Considering these possibilities, any single copy of your important data must always be considered at risk. That's why backing up is so important. Follow the 3-2-1 backup rule. Data should exist in three different places on two different storage media and at least one of those copies should be maintained offsite.

Without an effective backup strategy, recovering data may be impossible, or the cost of data recovery may be quite expensive. The CRU warranty does not cover costs associated with data loss (nor do the warranties of other data storage manufacturers).

Plan accordingly and backup data to minimize downtime!

## 10 Encryption

- The RAX212-3QR unit uses full disk hardware encryption to encrypt the entire contents of the drive—including the boot sector, operating system and all files—without performance degradation.
- The Security Key must be installed prior to powering on the RAX212-3QR unit for the data to be decrypted on the drive. If the key is externally connected to the Mini-USB Security Key Port and is not internally installed, then once it has been accepted, it may be removed and stored in a safe location. Always store Security Keys apart from the data so that in the event that the drive is lost or stolen, the data is protected.
- When a drive is formatted using an encryption key, the same or a duplicate key must be used in order to access the data. There is no “back door” to access the data; lost keys make data recovery virtually impossible.

## 11 Rack Mounting Warnings

**Elevated Operating Ambient Temperature:** The operating ambient temperature of the rack environment may be greater than the room ambient temperature if the unit is installed in a closed or multi-unit rack assembly. Install the equipment in an environment compatible with the maximum ambient temperature of 40° C.

**Reduced Air Flow:** Do not block or inhibit the air flow required for safe operation of the unit.

**Mechanical Loading:** Ensure that the unit is secure and level in the rack.

**Circuit Overloading:** Do not overload the circuits. Refer to the name plate ratings on the equipment.

**Reliable Grounding:** Maintain reliable grounding of rack-mounted equipment by using indirect connections to the branch circuit (i.e. UPS battery backups, power strips).

**Removing the Cover:** Turn off and unplug the unit before removing the cover.

## 12 Frequently Asked Questions

**Q:** Can I hot-swap drives with this product?

**A:** RAX Secure 3QR units support hot-swapping over USB and FireWire connections. If the eSATA/SATA host supports this feature, the drives can be hot-swapped via eSATA. Third-party host cards may or may not support this feature. Motherboard SATA connections often do not support hot swapping, so a discreet host card is recommended.

**Q:** I've attached my unit and can see the volume, but it shows up twice. Which one is real?

**A:** If you are seeing your volume mounted twice, chances are the product is connected to the computer using both the eSATA and FireWire connections. When this is the case, the OS may attempt to mount the unit twice, resulting in two volumes appearing. Simply turn off the unit and unplug one of the connections to resolve the problem.

**Q:** Why does my eSATA device appear as a Parallel SCSI device in Mac OS System Profiler?

**A:** The “Serial ATA” tab in System Profiler shows devices attached to the internal SATA bus, but not always devices attached to an eSATA host card. Sometimes these devices will appear under the heading “Parallel SCSI” instead. This is entirely normal and does not indicate a problem with the device or its drivers.

**Q:** Why is my hard drive experiencing data corruption?

**A:** Many things can cause data corruption on hard drives, whether they are inside your computer or inside an external storage product. Malicious software, OS bugs, failure to properly disconnect external devices, or for no apparent reason at all. Data corruption or loss is therefore not covered by warranty.

The first thing to try is to restart both the computer and the external device. If the data is still corrupted, try running built-in OS utilities on the hard drive (such as Mac OS X's Disk Utility First Aid or Windows' Check Disk tool with the setting “Scan for and attempt recovery of bad sectors” enabled).

If the OS utility doesn't help, you may need data recovery software. However, if there is a true hardware failure of your hard drive that prevents it from communicating with your computer, there is no software solution in existence that can fix this problem.

**Q:** Why won't the computer let me eject or unmount my drive?

**A:** There may be a software application running in the background with an active link to the drive. Sometimes, you may see a message such as “The disk is in use and could not be ejected. Try quitting applications and try again.”

This is not a defect or issue caused by the RAX Secure 3QR unit. Try invoking the Force Quit feature in OS X to see what software may be running. For Window, the equivalent command is CTRL+SHIFT+ESC.

Drives connected to the computer via eSATA cannot be ejected in Windows the way FireWire drives can. However, freeware utilities are available on the Internet that provide a similar function.

**Q:** Why can't I access my data when I turn on my unit?

**A:** If you have data on the drive, don't panic! Barring the failure of the hard drive your data is still intact, but is not reachable because the drive was not formatted within this unit using the correct Security Key. If you previously formatted the drive using a Security Key, power off the unit and insert the correct Security Key into the Mini-USB Security Key port on the front of the carrier. Then turn your unit back on. When both green LEDs are lit, showing that the drive is ready and encrypted, you should then be able to access your data. You can then remove the Security Key and store it in a safe location.

If you did not format the drive using a Security Key, you will need to make a backup copy of your data and format the drive using the correct Security Key. See Section 3 for instructions on how to format the drive with Mac or Windows operating systems.

**Q:** I turned my unit off and back on and now I cannot access my data. Why?

**A:** Cycling power on the unit will require you to reinsert the Security Key into the Mini-USB Security Key port before turning the unit back on, even if you have not turned your computer off. If the unit is on, power it off and insert the correct Security Key into the Mini-USB Security Key port on the front of the carrier. Then turn your unit back on. When both green LEDs are lit, showing that the drive is ready and encrypted, you should then be able to access your data. You can then remove the Security Key and store it in a safe location.

**Q:** Why can't I use another device through the Mini-USB port on the front of the DataPort SecureDock carrier?

**A:** This port is used by the Security Key to provide the encryption key to the unit hardware that will allow the unit to access the data on your hard drive. It does not pass data to the drive itself. Under no circumstances should you insert anything other than a Security Key into the Mini-USB Security Key Port. Though it is mechanically identical to the standard Mini-USB port, inserting a Mini-USB cable or other device into the Mini-USB Security Key Port on the carrier can cause internal

damage and potentially lead to loss of data.

Likewise, inserting the Security Keys into any other Mini-USB port will damage the keys and render them useless. Please only use the Security Keys in DataPort Secure products.

If you have already tried to use another device through this port or have inserted the Security Key into another device's Mini-USB port, first check to see if your Security Key still works in your DataPort SecureDock. If it does not, please contact Technical Support.

### 11.1 Contacting Technical Support

Still need help? Please contact our Technical Support team through [cru-inc.com/support](http://cru-inc.com/support). Call us toll free at (800) 260-9800 or directly at (360) 816-1800.

## 13 Technical Specifications

Product Models	RAX Secure 212-3QR
Interface Types & Speeds	<ul style="list-style-type: none"> <li>• USB 3.0: up to 1.5 Gbps</li> <li>• USB 2.0: up to 480 Mbps</li> <li>• eSATA: up to 1.5 Gbps</li> <li>• FireWire 800: up to 800 Mbps</li> </ul>
Drive Types Supported	2.5-inch and 3.5-inch SATA Hard Drives
Data Connectors	<ul style="list-style-type: none"> <li>• One (1) USB 3.0/2.0 connector</li> <li>• One (1) eSATA connector</li> <li>• Two (2) FireWire 800 connectors</li> </ul>
RAID Levels	JBOD, 0, 1
Encryption	256-bit AES (Advanced Encryption Standard)
Operating System Requirements	<ul style="list-style-type: none"> <li>• Windows 8.1, 7, Vista, or XP</li> <li>• Windows Server 2012, 2008, or 2003 product families</li> <li>• Mac OS X 10.4.x or higher</li> <li>• Linux distributions that support the connection type used</li> </ul>
Compliance	EMI Standard: FCC Part 15 Class A, CE EMC Standard: EN55022, EN55024
Shipping Weights	<ul style="list-style-type: none"> <li>• 17 pounds without drives (includes accessories)</li> <li>• 23 pounds with drives</li> </ul>
Product Dimensions	16.89" x 16.26" x 1.73" (429mm x 413mm x 44mm)
Technical Support	Your investment in CRU products is backed up by our free technical support for the lifetime of the product. Contact us through our website, <a href="http://cru-inc.com/support">cru-inc.com/support</a> or call us at 1-800-260-9800 or +1-360-816-1800.

© 2014 CRU Acquisition Group LLC. ALL RIGHTS RESERVED. RAX® and CRU® are trademarks of CRU Acquisition Group, LLC and are protected by trademark law.

### Product Warranty

CRU warrants this product to be free of significant defects in material and workmanship for a period of three years from the original date of purchase. CRU's warranty is nontransferable and is limited to the original purchaser.

### Limitation of Liability

The warranties set forth in this agreement replace all other warranties. CRU expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CRU dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CRU or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CRU product or service, even if CRU has been advised of the possibility of such damages. In no case shall CRU's liability exceed the actual money paid for the products at issue. CRU reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at this own expense.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

- 1) Ensure that the case of your attached drive is grounded.
- 2) Use a data cable with RFI reducing ferrites on each end.
- 3) Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
- 4) Reorient or relocate the receiving antenna.

